U.S. Department of Housing and Urban Development

Office of Policy Development & Research

Veterans Homelessness Prevention Study Data Files

Privacy Impact Assessment

FEBRUARY 13, 2012

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for the Veterans Homelessness Prevention Study Data Files. This document has been completed in accordance with the requirement set forth by the E-Government Act of 2002 and OMB Memorandum 03-22 which requires that "Privacy Impact Assessments" (PIAs) be conducted for all new and/ or significantly altered IT Systems, and Information Collection Requests.

ENDORSEMENT SECTION

Please check the appropriate statement.

X **The document is accepted.**
_____ **The document is accepted pending the changes noted.**
_____ **The document is not accepted.**

Based on our authority and judgment, the data captured in this document is current and accurate.

/Elizabeth Rudd/ **11/1/2011**
SYSTEM OWNER, ELIZABETH RUDD **Date**
OFFICE OF POLICY DEVELOPMENT & RESEARCH

/Carol Star/ **11/1/2011**
PROGRAM AREA MANAGER, CAROL STAR **Date**
DIRECTOR, PROGRAM EVALUATION DIVISION

/Harold Williams/ **03/15/2012**
DEPARTMENTAL PRIVACY ACT OFFICER **Date**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

TABLE OF CONTENTS

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
Veterans Homelessness Prevention Study Data Files
December 7, 2011

NOTE: See Section 2 for PIA answers, and Section 3 for Privacy Act Officer's determination.

SECTION 1: BACKGROUND

Importance of Privacy Protection – Legislative Mandates:

HUD is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, beneficiaries of HUD programs, business partners, and its own employees. These people have a right to expect that HUD will collect, maintain, use, and disseminate identifiable personal information only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- Privacy Act of 1974, as amended affords individuals the right to privacy in records that are maintained and used by Federal agencies. (See http://www.usdoj.gov/foia/privstat.htm);
- Computer Matching and Privacy Protection Act of 1988 is an amendment to the Privacy Act that specifies the conditions under which private information may (or may not) be shared among government agencies. (See http://www.usdoj.gov/foia/privstat.htm);
- Freedom of Information Act of 1966, as amended (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy. See also HUD's Freedom of Information Act Handbook (HUD Handbook 1327.1 at www.hudclips.org);
- E-Government Act of 2002 requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf; see also the summary of the E-Government Act at http://www.whitehouse.gov/omb/egov/pres_state2.htm);
- Federal Information Security Management Act of 2002 (which superceded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security regulations at Title 44 U.S. Code chapter 35 subchapter II (http://uscode.house.gov/search/criteria.php); and
- OMB Circular A-130, Management of Federal Information Resources, Appendix I (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those staff that have a need to access the data to carry out their duties; and they will be held accountable for ensuring privacy and confidentiality of the data.

What is the Privacy Impact Assessment (PIA) Process?

The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: http://www.hud.gov/offices/cio/privacy/pia/pia.cfm. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN + birth date + financial information would pose more risk to privacy than just name + SSN alone.

The PIA:

- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?

Both the program area System Owner and IT Project Leader work together to complete the PIA. The System Owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT Project Leader describes whether technical implementation of the System Owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

1. New Systems: Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).

2. Existing Systems: Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA): Agencies must obtain OMB approval for new information collections from ten or more members of the public. If the information collection is both a new collection and automated, then a PIA is required.

What are the Privacy Act Requirements?

Privacy Act. The Privacy Act of 1974, as amended (http://www.usdoj.gov/foia/privstat.htm) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is the PIA Summary Made Publicly Available?

The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD's Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD's web site. See: http://www.hud.gov/offices/cio/privacy/pia/pia.cfm.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Act Officer in the Office of the Chief Information Officer (OCIO). If any question does not apply, state Not Applicable (N/A)

Program Area: Program Evaluation Division, RRE, Office of Policy Development & Research
Subject matter expert in the program area: Elizabeth Rudd, Office of Policy Development and Research, Program Evaluation Division, 202-402-7607
Program Area Manager: Carol S. Star, Office of Policy Development and Research, Program Evaluation Division, (202) 402-6139
IT Project Leader: N/A, not an internal HUD system so no IT Project Leader

For IT Systems:

- **Name of system:** Veterans Homelessness Prevention Demonstration Evaluation Data Files
- **PCAS #:** N/A
- **OMB Unique Project Identifier #:** N/A
- **System Code: N/A**
- **Development Date: N/A**
- **Expected Production Date: N/A**

For Information Collection Requests:

- **Name of Information Collection Request:** Evaluation of the Veterans Homelessness Prevention Demonstration
- **OMB Control #:** XXXXXX

Question 1: Provide a general description of the system that describes: (a) the personal information collected; (b) who does it pertain only to (i.e., government employees, contractors, or consultants); (c) the functionality of the system and the purpose that the records and/or system serve; (d) how information is transmitted to and from the system; (e) interconnections with other systems.

General description of the system: The dataset created by this study will enable evaluation of the Veterans Homelessness Prevention Demonstration (VHPD). The VHPD was mandated by Congress in the FY2009 budget, which included $10 million for the Department of Housing and Urban Development (HUD) to launch a homelessness prevention demonstration for veterans and directed HUD to collaborate with the Department of Veterans Affairs (VA) and the Department of Labor (DOL) to develop the demonstration. The VA designated $5 million for case management for the VHPD. HUD selected five military bases and surrounding communities to participate in VHPD: Camp Pendleton in San Diego, CA; Fort Hood in Killeen Texas; Fort Drum in Watertown, NY; Joint Base Lewis-McChord in Tacoma, WA; and MacDill Air Force Base in Tampa, FL. HUD demonstration funds were allocated directly to the largest Continuum of Care (CoC) in the geographic area covered by the VHPD programs: the City of San Diego; Austin/Travis County; Utica/Rome/Oneida County; Tacoma/Lakewood/ Pierce County; and Tampa/Hillsborough County. HUD awarded each grantee $2 million for a period of 3 years starting in February 2011. Grants went to homeless assistance programs in designated CoCs or

to the CoC itself, to deliver housing and supportive services in collaboration with VA medical centers (VAMCs) and DOL One-Stop workforce development centers. VHPD grantees and their subgrantees can provide a range of financial, case management, and housing location services to households that are homeless or at risk for homelessness.

(a) The personal information collected: The system will collect the personal information indicated in the table below.

(b) Who does the system pertain to? The system will include data about members of the public, including a sample of clients of the VHPD program, a sample of veterans who did not participate in the VHPD, and a sample of non-veterans who participated in a different homelessness prevention program (Homelessness Prevention and Rapid Re-housing).

(c) The functionality of the system and the purpose that the records and/or system serve: The purpose of the data collected is to allow measurement of the efficacy of the VHPD. HUD contracted with Silber & Associates and the Urban Institute to conduct the evaluation, which is congressionally mandated. Two types of data will be collected: (1) survey data collected directly from the participant; and (2) administrative data from grantees, subgrantees, local homelessness organizations, CoCs, or VAMCs. The sample includes the following groups:

- *Group 1:* 500 VHPD program participants—HUD will collect a baseline and follow up survey, and administrative data.
- *Group 2:* Comparison group of 500 Veterans who would have qualified for VHPD, but did not participate in VHPD—HUD will collect administrative data.
- *Group 3:* Comparison group of non-veteran HPRP participants –HUD will collect administrative data only.

(d) How information is transmitted to and from the system: All survey data will be collected through telephone interviews and compiled by Silber & Associates. The dataset will be de-identified by Silber & Associates and then transmitted either via mail on a medium that is password protected and encrypted or via a secure FTP site to the Urban Institute. Administrative data will be transmitted by mail or electronically using the same safeguards. See below for a more detailed discussion of physical safeguards during transmission. Confidentiality of personal identifying information (PII) collected for this study will be maintained through a combination of management, operational, and technical controls, which are defined broadly in NIST SP 800-53, and are the basis of HUD's policies as defined in HUD Information Technology Security Policy, Handbook 2400.25 Rev. 1. Please see "other comments" at the end of this document for a full description of the Data Security Plan pertaining to the Evaluation of the Veterans Homelessness Prevention Demonstration.

(e) Interconnections with other systems: The Veterans Homelessness Prevention Demonstration Evaluation Data Files will be a stand-alone system.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

Personal Identifiers:

X	Name
X	Social Security Number (SSN). Specify the purpose/legal authority authorizing the solicitation of SSNs (This includes truncated SSNs): SSNs are required to match the participant study records with other already existing administrative data sets for purposes of assessing client outcomes.
X	Other identification number (specify type): Participant Study Unique ID #: This ID # will be a randomly generated unique ID that will allow the research team to create "de-identified" files that link the unique id to study data without using personal identifiers.
X	Birth date
X	Home address
X	Home telephone
X	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
	Comment:

Personal/ Sensitive Information:

X	Race/ ethnicity
X	Gender/ sex
X	Marital status
X	Spouse name
X	# of children
X	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.): Earned income, benefit receipt (e.g. SSI, SSDI, TANF, etc.), assets.
X	Employment history
X	Education level
X	Medical history/ information
X	Disability
X	Criminal record
X	Other (specify): residential history, homeless program utilization, barriers to housing, veteran status; contact information for up to three relatives or friends for future follow-up.

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, proceed to answering the following questions.	☒	☐
Have the security controls been reviewed and approved by the Information Security Officer?	☒	☐

What security controls are in place to protect the information (e.g., encryptions)?

All personal data (in both identifiable and de-identified data files) will be encrypted and maintained on a secure workstation or server that is protected by a firewall and multi-authenticated passwords in a directory that can only be accessed by the network administrators and the research team. Access to personally identifiable information will be restricted to a very small number of staff who have a need to access the data to carry out their duties; they will be held accountable for ensuring privacy and confidentiality of the data.

Physical safeguards during transmission

All survey data (including pre-test interviews) will be collected and compiled by Silber & Associates, who will present a complete and de-identified dataset to the Urban Institute. Silber & Associates will create two datasets, the Master File will contain a unique identifier for each survey respondent (the Participant Study Unique ID) and personal identifying information, but none of the other study data. The second dataset, the Study File, will contain the Participant Study Unique IDs and the study data, but it will NOT contain name, social security number, birth date, home address, home telephone or personal email address. The Study File will be de-identified. The purpose of the Study File is to provide Urban Institute researchers with de-identified data for analysis. The Master File will be stored securely by Silber & Associates. It will only be used when necessary for follow-up contacts and linking data from multiple agencies. The Study File, which will be de-identified, will be transmitted to the Urban Institute to be used for data analysis.

For administrative data, the Urban Institute will create data sharing agreements with participating agencies.

If survey or administrative data are mailed, they will be sent to the Urban Institute via a shipping service that provides tracking information. If administrative or survey data are transferred via a secure FTP site, UI will download them to encrypted hard-drives only. Electronic media will be password protected and encrypted. If data arrive with personally identifying information, the file (in any form, hard copy, tape, diskette) is stored in a locked file which can be accessed only by staff who have signed a Staff Confidentiality Pledge. However, we do not anticipate transmission of personally identifiable data collected for the VHPD Evaluation.

At the Urban Institute, data files will be stored on a secure network drive that can only be accessed by project staff for data analysis.

What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? Remote login at the Urban Institute is protected SSL VPN. Silber & Associates will not allow remote access to the VHPD Evaluation Data Files.
Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbucks) or is remote access permitted from all areas outside the Department? Remote access to the Study File is permitted only from approved, secure computers, such as an employee's approved alternative work station or laptop. Remote access to the Master File, which is stored at Silber & Associates, is prohibited.
Is there a policy that identifies "if" or "if not" downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)? The data security plan prohibits downloading data and remote storage.
Comment:

Question 3: Type of electronic system or information collection.

A. If this is a new electronic system (or one in development) (implemented after April 2003, the effective date of the E-Government Act of 2002)?	**Yes** ☒	**No** ☐
Does the system require authentication? Yes, it requires complex password, multi-factor authentication.	☒	☐
Is the system browser-based? No, the study dataset will not be browser-based.	☐	☒
Is the system external-facing (with external users that require authentication)? Yes.	☒	☐

B. If this is an existing electronic system has the system undergone any changes (since April 17, 2003)**?** If an existing system, when was the system developed? _____	**Yes** ☐	**No** ☐
Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?	☐	☐

Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?	☐	☐
If yes, please explain:		

C. For your new and/or existing electronic system, please indicate if any of the following changes have occurred: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA or PIA update (if not applicable, mark N/A):	
	Conversion: When paper-based records that contain personal information are converted to an electronic system
	From Anonymous (Non-Identifiable) to "Non-Anonymous" (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new "relational" databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
	New Public Access: When new public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)
	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

D. If an Information Collection Request (ICR): Is this a new Request that will collect data that will be in an automated system? Agencies must obtain OMB approval

for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a new request and the collected data will be in an automated system.	
X	Yes, this is a new ICR and the data will be automated
	No, the ICR does not require a PIA because it is not new or automated)
	Comment:

Question 4: Explain by Line of Business why the personally identifiable information is being collected? How will it be used?

The FY 2009 budget for the U.S. Department of Housing and Urban Development included a $10 million set-aside to implement a Veterans Homelessness Prevention Demonstration (VHPD). As outlined in the VHPD Notice of Funding Availability (NOFA), HUD is responsible for "conducting an evaluation of the demonstration program and grantees must agree to participate in the evaluation." To measure the effectiveness of the program, HUD's contractors, Silber & Associates and the Urban Institute, will conduct a process and outcomes study. The outcomes study will follow 500 VHPD participants and two comparison groups of 500 each, including a group of veterans who did not receive VHPD services and a group of non-veterans who received homelessness prevention services through a different program (Homelessness Prevention and Rapid Re-Housing). The study will use survey and administrative data to examine reductions in shelter entry and improvements in housing stability, as well as changes in employment and earnings, self-sufficiency, and overall well-being and health.

Participation in the study is voluntary. Verbal consent will be collected for participation in the survey (baseline and follow up) and written consent will be collected for all administrative data accessed by the research team. Information will be secured through a combination of management, operational, and technical controls, which are defined broadly in NIST SP 800-53, and are the basis of HUD's policies as defined in HUD Information Technology Security Policy, Handbook 2400.25 Rev. 1.

Mark any that apply:

Homeownership:

	Credit checks (eligibility for loans)
	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	Loan default tracking
	Issuing mortgage and loan insurance
	Other (specify):
	Comment:

Rental Housing Assistance:

	Eligibility for rental assistance or other HUD program benefits
	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
	Other (specify):
	Comment:

Grants:

	Grant application scoring and selection – if any personal information on the grantee is included
	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

Internal operations:

	Employee payroll or personnel records
	Payment for employee travel expenses
	Payment for services or products (to contractors) – if any personal information on the payee is included
	Computer security files – with personal information in the database, collected in order to grant user Ids
	Other (specify):
	Comment:

Other lines of business (specify uses):

x	Research data compilation and analysis

Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)?

Mark any that apply:

	Federal agencies?
	State, local, or tribal governments?

	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	HUD module/application? (specify the module(s)/application(s) name)
	Others? (specify): The research data will be collected by researchers of Silber & Associates (S&A) and the Urban Institute (UI), both firms are under contract to HUD to collect the data. The data will be shared only for research purposes, as detailed in the System of Records Notice for this data collection. Therefore, the data may be shared with PD&R researchers, contract researchers, consultants, and grantees, when relevant, to analyze data, including statistical analysis, and write reports to advance the goals of the nation's federal strategic plan to prevent and end homelessness. The data will only be shared with authorized researchers, who have signed statements agreeing to abide by all necessary measures to ensure data confidentiality. Except for a few selected researchers who need access to PII in order to fulfill the research plan, PII will not be shared with researchers; researchers will work with de-identified data. Survey and administrative data will be stored on a secure, password protected network drive. Only personnel authorized by the project director will be given access. Access is limited by using technical controls based on policies administered by the system administrator. Authorized personnel accessing the data through the survey system are monitored through a secured restricted access monitoring system, which is FIPS compliant. S&A and UI servers are protected by endpoint protection and firewall access controls and policies that provide access to authorized personnel only. S&A and UI desktop systems accessing secured data have full disk encryption and are protected by endpoint protection software and a client firewall policy. Furthermore, S&A and UI desktops are password protected and employees must comply with policies that control access. At both S&A and UI physical access to secured data rooms is restricted to authorized IT personnel and authorized project staff. Recorded information is kept on an encrypted system with endpoint protection and access control policies for authorized personnel. At S&A, data are backed up daily. Only authorized personnel can access recordings over a secured connection. Authorized users are allowed access with user name and password. The system resides on the premises and is accessible only by the project director and staff authorized by the director. At UI, data files will be stored on a secure network drive that can only be accessed by project staff who need access to conduct data analysis. Data files will be backed up manually to dvd that will be kept in a locked drawer. Upon completion of the project, dvd(s) containing data files will be destroyed, as follows: Data with personal identifiers will be maintained only as long as required and only under conditions

	specified in the study protocol. Within 6 months of study completion, S&A will permanently destroy all electronic personally-identifiable information on the working server using one of the methods described by the NIST SP 800-88 "Guidelines for Media Sanitization" (September 2006). Encrypted versions of the data may remain on backup media for a longer period of time, but will be similarly permanently destroyed. At the end of the contract, dvd(s) and hardcopy records that do not need to be retained will be shredded and the remainder of the files will be shredded after the three-year retention period required in the contract.
	Comment:

Question 6: Can individuals "opt-out" by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

X	Yes, individuals can "opt-out" by declining to provide private information or by consenting only to particular use
	No, they can't "opt-out" – all personal information is required
	Comment:

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

Participation in the study is voluntary. There are no risks to veterans participating in the study and no risks associated with refusing to participate in the study. Participation in the study will not affect services or benefits they may receive or be eligible to receive. Participants may opt out of the study at any point in time, for any reason, with no consequences.

Question 7: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?

Mark any that apply and give details if requested:

X	**System users must log-in with a password (Please specify password type):** complex password and multi-factor authentication by authorized research personnel

X	**When an employee leaves:** • **How soon is the user ID terminated?** 1 day (1 day, 1 week, 1 month, unknown)? • **How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve):** As part of employee termination process, user IDs are terminated, VPN access is terminated, the authentication security card must be returned, and an employee termination worksheet documenting these steps is completed.
X	**Are access rights selectively granted, depending on duties and need-to-know?** Yes. **If Yes, specify the approximate # of authorized users who have either:** • Full access rights to all data in the system: Approximately 3 Limited/restricted access rights to only selected data: ▪ Approximately 4 Silber & Associates/Urban Institute researchers with access to data collected directly from participating families across all sites. ▪ Approximately 4 Silber & Associates/Urban Institute researchers with access to data collected directly from participating veterans in the site in which he/she is collecting data; that is, each of these individuals will only have access to the data in one site. ▪ Approximately 2 Silber & Associates/Urban Institute researchers with access to de-identified individual-level data. Each researcher will sign a data security and participant confidentiality protocol that outlines the data security plan for the study. Each researcher will be assigned access to the data based on their specific role in the project.
X	**Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve):** Yes. The research staff will securely store any hard copy documents and diskettes with study data with personal protected information. At Silber & Associates survey and administrative data (hard copies and diskettes) will be stored in the project director's locked file cabinet. At UI, data will be stored in the task leader's locked file cabinet.
	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve: N/A

	Other methods of protecting privacy (specify):
	Comment:

Question 8: If <u>privacy</u> information is involved, by what data element(s) is it retrieved from the system?

Mark any that apply

X	Name:
X	Social Security Number (SSN)
X	Identification number (specify type):
X	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
	None
	Comment:

Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the Federal Register to cover this system? Yes ☐ No ☒ (Please consult with your component's Privacy office if assistance is needed in responding to this question.)

The Privacy Act System of Records Notice (SORN) has been drafted and is pending review by Privacy Office before publication.

If yes, provide the Federal Register citation

Other Comments (or details on any Question above):

The Data Security plan is included here.

Introduction

The FY 2009 budget for the U.S. Department of Housing and Urban Development included a $10 million set-aside to implement a Veterans Homelessness Prevention Demonstration (VHPD) targeting early intervention homelessness prevention primarily to veterans returning from Iraq and Afghanistan. According to the VHPD Notice of Funding Availability (NOFA), HUD is responsible for "conducting an evaluation of the demonstration program and grantees must agree to participate in the evaluation." Silber & Associates and the Urban Institute (S&A/UI) will conduct a study to measure the effectiveness of the program. The study will use survey and administrative data to examine whether program the program leads to reductions in shelter entry and improvements in housing stability, as well as investigating changes in employment and earnings, self-sufficiency, and overall well-being and health.

S&A and UI are research firms with extensive experience storing, safeguarding and, finally, destroying personally identifiable information. Both organizations have developed policies, procedures, standards, and guidelines for data security that meet HUD's standards for data security. This data security plan describes how data collected for the VHPD evaluation will be handled, stored, and destroyed. S&A is certified as in compliance with Federal Information Processing Standards (FIPS) 140-2 compliant, i.e., compliant with the government standards that specify best practices for implementing crypto algorithms, handling key material and data buffers, and working with the operating system.[1] Certification is by independent third party. S&A will collect and store personally identifiable data and provide UI with a de-identified dataset for use in data analysis.

1. Data Consent

Survey. S&A will administer a baseline and follow-up survey via telephone to VHPD participants. The site will receive written consent from participants at the time of program enrollment to provide contact information so that the research team can contact participants for survey participation. Participation is voluntary. S&A interviewers will obtain oral consent before proceeding with the survey. VHPD participants may decline participation at any time without repercussions.

Administrative Data. The S&A/UI team will collect administrative data from local Homeless Management Information Systems (HMIS) and VA Medical Centers and Facilities. Participants will provide written consent for all data collected that includes personal identifiers. Depending on the study site, consent for collecting this data will be provided through one of the following vehicles: (a) a written consent form signed by the participant specifically for this study or (b) a written consent to share information for research purposes provided to the agency and signed by the participant.

2. Data Access

Access to personally identified data will be limited to members of the research team who have a need for the information to do their jobs. All team members will be advised of the data security requirements and will agree to them in writing prior to working with the study data.

There will be no remote access of personally identified data.

Remote access to data for analysis will be limited to UI researchers working with a de-identified dataset and working from an approved, secure computer such as the employee's approved alternative workstation or laptop. Remote access will only be permitted for data files that do not include personal identifiers. UI remote login is protected by SSL VPN.

3. Data Storage

[1] Federal Information Processing Standard 140-1 (FIPS 140-1) and it successor FIPS 140-2 are U.S. Government standards that provide a benchmark for implementing cryptographic software. They specify best practices for implementing crypto algorithms, handling key material and data buffers, and working with the operating system.

Survey and administrative data will be stored on a secure, password protected network drive. Only personnel authorized by the project director will be given access. Access is limited by using technical controls based on policies administered by the system administrator. Authorized personnel accessing the data through the survey system are monitored through a secured restricted access monitoring system, which is FIPS compliant. S&A and UI servers are protected by endpoint protection and firewall access controls and policies that provide access to authorized personnel only. S&A and UI desktop systems accessing secured data have full disk encryption and are protected by endpoint protection software and a client firewall policy. Furthermore, S&A and UI desktops are password protected and employees must comply with policies that control access. At both S&A and UI physical access to secured data rooms is restricted to authorized IT personnel and authorized project staff. Recorded information is kept on an encrypted system with endpoint protection and access control policies for authorized personnel.

At S&A, data are backed up daily. Only authorized personnel can access recordings over a secured connection. Authorized users are allowed access with user name and password. The system resides on the premises and is accessible only by the project director and staff authorized by the director.

At UI, data files will be stored on a secure network drive that can only be accessed by project staff who need access to conduct data analysis. Data files will be backed up manually to dvd that will be kept in a locked drawer. Upon completion of the project, dvd(s) containing data files will be destroyed, as outlined in Section 5.

4. Data Transmission

All survey data (including pre-test interviews) will be collected and compiled by S&A, who will present a complete and de-identified dataset to UI for analysis. S&A will create two datasets, the Master File will contain a unique identifier for each survey respondent (the Participant Study Unique ID) and personally identifying information, but none of the other study data. The second dataset, the Study File, will contain the Participant Study Unique IDs and the study data, but it will NOT contain name, social security number, birth date, home address, home telephone or personal email address. In other words, the Study File will be de-identified. The purpose of the Study File is to provide UI researchers with de-identified data for analysis. The Master File will be stored securely by S&A. It will only be used when necessary for follow-up contacts and linking data from multiple agencies. The Study File, which will be de-identified, will be transmitted to UI to be used for data analysis.

If survey or administrative data are mailed to UI, they will be sent via a shipping service that provides tracking information. If administrative or survey data are transferred via a secure FTP site, UI will download them to encrypted hard drives only. Electronic media will be password protected and encrypted. It is UI's general policy that if data arrive with personally identifying information, the file (in any form, hard copy, tape, diskette) is stored in a locked file, which can be accessed only by staff who have signed a Staff Confidentiality Pledge. However, for the VHPD study UI does not anticipate receiving data with personally identifying information.

For use of administrative data, the UI will create data sharing agreements with participating agencies, which will ensure the confidentiality and security of the data. S&A will manage the process of matching survey data with administrative data. The UI will not need to receive administrative data with personal identifiers.

5. Data Disposal

Data with personal identifiers will be maintained only as long as required and only under conditions specified in the study protocol. Within 6 months of study completion, S&A will permanently destroy all electronic personally-identifiable information on the working server using one of the methods described by the NIST SP 800-88 "Guidelines for Media Sanitization" (September 2006). Encrypted versions of the data may remain on backup media for a longer period of time, but will be similarly permanently destroyed. At the end of the contract, dvd(s) and hardcopy records that do not need to be retained will be shredded and the remainder of the files will be shredded after the three-year retention period required in the contract.

6. Staff Confidentiality Agreements

Access to data will be limited to research team members at UI and S&A who need access for purposes of the VHPD evaluation research and who have agreed in writing to maintain the confidentiality of all data.

All employees of S&A and UI are required to sign a confidentiality pledge as a condition of employment and breach of that agreement is grounds for immediate termination.

7. Protocol for Reporting Critical Incidents

All serious, adverse events and unanticipated problems or adverse events that represent an increase in severity or frequency of the known risks of participation in this study will be reported to the S&A project director immediately. A formal written incident report will be provided to the client within ten (10) working days of the discovery of the incident. An adverse event is considered to be a serious adverse event (SAE) if the event results in or requires medical or surgical intervention to prevent any of the following outcomes: death, a life-threatening situation, hospitalization or prolongation of existing hospitalization, a persistent or significant disability or incapacity, a congenital anomaly or birth defect. A serious adverse event may be related or unrelated to the research and is usually unanticipated.

8. Data Reporting

Project findings and reports prepared for dissemination will not contain information that could reasonably be expected to be used to identify an individual.

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER